

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-8. **(Canceled)**

9. **(Previously Presented)** An apparatus comprising:

at least a first application;

an authentication component configured to authenticate a communicating device;

an access control component accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication component, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control component configured to instruct the authentication component to authenticate the communicating device, wherein the access control component is configured to receive indications originating from the communicating device identifying the communicating device and the application requested; and

wherein the authentication component is configured to authenticate the communicating device by verifying an identity of the communicating device or by verifying a personal identification number.

10-26. **(Canceled)**

27. **(Previously Presented)** An apparatus comprising:

at least first and second applications;

an authentication component configured to authenticate a communicating device;

a first access control component accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication component, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control

component configured to instruct the authentication component to authenticate the communicating device;

a second access control component accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication component, and arranged to arbitrate whether access of the communicating device to the second application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the second access control component configured to instruct the authentication component to authenticate the communicating device, wherein the first access control component is accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication component, and is arranged to provide the access of the communicating device to the second access control component; and

wherein the authentication component is configured to authenticate the communicating device by verifying an identity of the communicating device or by verifying a personal identification number.

28. **(Canceled)**

29. **(Previously Presented)** An apparatus comprising:

a processor; and

a memory having stored therein machine executable instructions, that when executed, cause the apparatus to:

receive, from a requesting device, a request at the apparatus and passing it, without authenticating the requesting device, to an arbitration component interfacing the service;

determine, in the arbitration component, whether to grant or refuse access to the first application to the requesting device, wherein if the determination requires an authentication of the requesting device, the authentication is performed during that determination and not previously, wherein the determination is made on the basis of the identity of service requested and/or the identity of the requesting device; and

wherein authentication includes verifying an identity of the requesting device or verifying a personal identification number.

30. **(Withdrawn)** A device for providing services and allowing access by other devices to the provided services, comprising:

an interface for communicating with the other devices and receiving requests to access a service therefrom;

arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication, originating from the other device, identifying the other device, wherein, if the requesting device has a stored trust indication associated therewith no user authorization is required and if the requesting device has no stored trust indication associated therewith user authorization is requirable; and

a user interface for providing user authorization.

31. **(Withdrawn)** A device for providing services and allowing access by other devices to the provided services, comprising:

an interface for communicating with the other devices and receiving requests to access a service therefrom;

arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and store security indications in association with provided services and arranged to receive from the interface indications, originating from the other device, identifying the other device and the service requested, wherein, if the requesting device has a stored trust indication associated therewith no user authorization is required and if the requesting device has no stored trust indication associated therewith user authorization is required in dependence upon the stored security indication associated with the requested service;

and a user interface for providing user authorization.

32. **(Canceled)**

33. **(Previously Presented)** The apparatus as claimed in claim 9 wherein the access control component is arranged to store security indications in association with accessible applications, wherein a stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration.

34. **(Previously Presented)** The apparatus as claimed in claim 33 wherein the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration, in independence of the identity of the communicating device.

35. **(Previously Presented)** The apparatus as claimed in claim 9 further comprising a user interface configured to authorize access to an application during arbitration, the access control component being arranged to store security indications in association with accessible applications, wherein a stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration.

36. **(Previously Presented)** The apparatus as claimed in claim 35 wherein the access control component is further arranged to store trust indications in association with devices, and wherein the stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration in dependence upon any stored trust indication associated with the communicating device.

37. **(Previously Presented)** The apparatus as claimed in claim 9 wherein authentication comprises secret key exchange between the apparatus and the communicating device.

38. **(Previously Presented)** The apparatus as claimed in claim 29 wherein the instructions further cause the apparatus to:

store security indications in association with accessible applications, wherein a stored security indication associated with the first application is indicative of whether authentication of the requesting device is or is not required during arbitration.

39. **(Previously Presented)** The apparatus as claimed in claim 38 wherein the stored security indication associated with the first application is indicative of whether authentication of the requesting device is or is not required during arbitration, in independence of the identity of the requesting device.

40. **(Previously Presented)** The apparatus as claimed in claim 29 wherein the instructions further cause the apparatus to:

authorize access to an application during arbitration via a user interface, and storing security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration.

41. **(Previously Presented)** The apparatus as claimed in claim 40 wherein the instructions further cause the apparatus to:

store trust indications in association with devices, and wherein the stored security indication associated with the first application is indicative of whether user authorization of the requesting device is or is not required during arbitration in dependence upon any stored trust indication associated with the requesting device.

42. **(Previously Presented)** The apparatus as claimed in claim 29 wherein authentication comprises secret key exchange between the providing device and the requesting device.

43. **(Previously Presented)** A method comprising:

receiving, by a providing device, a request to access an application and passing it, without authenticating a requesting device, to an arbitration component interfacing a service;

determining, by the providing device, in the arbitration component, whether to grant or refuse access to the application, said determining including an authentication of the requesting device, said authentication performed during the determination and not previously, wherein the determination is made on the basis of the identity of the application requested; and

wherein authentication includes verifying an identity of the requesting device or verifying a personal identification number.

44. **(Previously Presented)** The method of claim 43 wherein the determination is made on the basis of the identity of the requesting device.

45. **(Previously Presented)** The method as claimed in claim 43, comprising storing security indications in association with accessible applications, wherein a stored security indication associated with the application is indicative of whether authentication of the requesting device is or is not required during arbitration.

46. **(Previously Presented)** The method as claimed in claim 45 wherein the stored security indication associated with the application is indicative of whether authentication of the requesting device is or is not required during arbitration, in independence of the identity of the requesting device.

47. **(Previously Presented)** The method as claimed in claim 43 further comprising authorizing access to the application during arbitration via a user interface, and storing security indications in association with accessible applications, wherein a stored security indication associated with the application is indicative of whether user authorization of the requesting device is or is not required during arbitration.

48. **(Previously Presented)** The method as claimed in claim 47 comprising storing trust indications in association with devices, and wherein the stored security indication associated with the application is indicative of whether user authorization of the requesting device is or is not required during arbitration in dependence upon any stored trust indication associated with the requesting device.

49. **(Previously Presented)** The method as claimed in claim 43 wherein authentication comprises secret key exchange between the providing device and the requesting device.

50. **(Previously Presented)** The apparatus as claimed in claim 27, wherein the first access control component and the second access control component are arranged to store security indications in association with accessible applications, wherein a first stored security indication

associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration and wherein a second stored security indication associated with the second application is indicative of whether authentication of the communicating device is or is not required during arbitration.

51. **(Currently Amended)** A non-transitory machine accessible and readable medium tangible computer readable storage medium encoded with instructions, when executed by a processor, cause the processor to perform:

receiving a request to access an application and passing it, without authenticating the requesting device, to an arbitration component interfacing the service;

determining, in the arbitration component, whether to grant or refuse access to the application, wherein if the determination requires an authentication of the requesting device, the authentication is performed during that determination and not previously, wherein the determination is made on the basis of the identity of the application requested; and

wherein authentication includes verifying an identity of the requesting device or verifying a personal identification number.

52. **(Currently Amended)** The non-transitory machine accessible and readable medium computer readable storage medium as claimed in claim 51, encoded with instructions, when executed by the processor, further cause the processor to perform:

storing security indications in association with accessible applications, wherein the stored security indication associated with an application is indicative of whether authentication of the requesting device is or is not required during arbitration.

53. **(Canceled)**

54. **(Previously Presented)** The apparatus of claim 9, wherein the apparatus is configured to receive a personal identification number (PIN) and calculate a temporary initial authentication link key using the received personal identification number (PIN).

55. **(Previously Presented)** The apparatus of claim 27, wherein the authentication component is configured to authenticate the communicating device by verifying an identity of the communicating device or by verifying a personal identification number.

56. **(Previously Presented)** The apparatus of claim 27, wherein the apparatus is configured to receive a personal identification number (PIN) and calculate a temporary initial authentication link key using the received personal identification number (PIN).

57. **(Canceled)**

58. **(Previously Presented)** The method of claim 43, further comprising receiving a personal identification number (PIN) and calculating a temporary initial authentication link key using the received personal identification number (PIN).